

Nombres de Carmichael

Marc Lorenzi

15 juillet 2026

1 Introduction

Pour tout $n \in \mathbb{N}^*$, notons $\mathbb{Z}_n$ l'anneau des entiers modulo n et $\mathbb{Z}_n^\times$ le groupe des éléments inversibles de l'anneau $\mathbb{Z}_n$. Le groupe $\mathbb{Z}_n^\times$ est de cardinal $\varphi(n)$ où φ est la fonction indicatrice d'Euler. Le *petit théorème de Fermat* nous dit que si n est premier, alors pour tout $a \in \mathbb{Z}_n^\times$, $a^{n-1} = 1$. Nous allons dans cet article nous intéresser aux entiers n *composés* qui vérifient encore cette propriété.

Définition 1. Soit $n \geq 2$. L'entier n est un *nombre de Carmichael* si n est composé et pour tout $a \in \mathbb{Z}_n^\times$, $a^{n-1} = 1$.

Proposition 1. Les nombres de Carmichael sont impairs.

Démonstration. Soit n un nombre de Carmichael. Supposons n pair. On a $n - 1$ impair, donc

$$(-1)^{n-1} = -1$$

Mais n est un nombre de Carmichael, donc

$$(-1)^{n-1} = 1$$

De là, $-1 = 1$ dans $\mathbb{Z}_n$, d'où $n = 2$. Contradiction, puisque 2 est premier. $\square$

Il existe 141 nombres de Carmichael inférieurs à 2×10^7 , qui sont

561	1105	1729	2465	2821	6601	8911	10585	15841	29341
41041	46657	52633	62745	63973	75361	101101	115921	126217	162401
172081	188461	252601	278545	294409	314821	334153	340561	399001	410041
449065	488881	512461	530881	552721	656601	658801	670033	748657	825265
838201	852841	997633	1024651	1033669	1050985	1082809	1152271	1193221	1461241
1569457	1615681	1773289	1857241	1909001	2100901	2113921	2433601	2455921	2508013
2531845	2628073	2704801	3057601	3146221	3224065	3581761	3664585	3828001	4335241
4463641	4767841	4903921	4909177	5031181	5049001	5148001	5310721	5444489	5481451
5632705	5968873	6049681	6054985	6189121	6313681	6733693	6840001	6868261	7207201
7519441	7995169	8134561	8341201	8355841	8719309	8719921	8830801	8927101	9439201
9494101	9582145	9585541	9613297	9890881	10024561	10267951	10402561	10606681	10837321
10877581	11119105	11205601	11921001	11972017	12261061	12262321	12490201	12945745	13187665
13696033	13992265	14469841	14676481	14913991	15247621	15403285	15829633	15888313	16046641
16778881	17098369	17236801	17316001	17586361	17812081	18162001	18307381	18900973	19384289
19683001									

Voici les factorisations des nombres de Carmichael inférieurs à 10^5 .

$$\begin{aligned}
561 &= 3 \times 11 \times 17 \\
1105 &= 5 \times 13 \times 17 \\
1729 &= 7 \times 13 \times 19 \\
2465 &= 5 \times 17 \times 29 \\
2821 &= 7 \times 13 \times 31 \\
6601 &= 7 \times 23 \times 41 \\
8911 &= 7 \times 19 \times 67 \\
10585 &= 5 \times 29 \times 73 \\
15841 &= 7 \times 31 \times 73 \\
29341 &= 13 \times 37 \times 61 \\
41041 &= 7 \times 11 \times 13 \times 41 \\
46657 &= 13 \times 37 \times 97 \\
52633 &= 7 \times 73 \times 103 \\
62745 &= 3 \times 5 \times 47 \times 89 \\
63973 &= 7 \times 13 \times 19 \times 37 \\
75361 &= 11 \times 13 \times 17 \times 31
\end{aligned}$$

Le nombre 41041 (qui est magiquement égal à 1001×41) est le plus petit nombre de Carmichael qui possède 4 facteurs premiers. Le plus petit nombre de Carmichael qui possède 5 facteurs premiers est

$$825265 = 5 \times 7 \times 17 \times 19 \times 73$$

Pour savoir comment j'ai obtenu ces nombres, lisez la suite.

2 Conditions nécessaires

Donnons nous un entier naturel n impair différent de 1. Écrivons

$$n = p_1^{e_1} \dots p_r^{e_r}$$

où $r \in \mathbb{N}^*$, les p_i sont des nombres premiers impairs distincts et les e_i sont des entiers non nuls.

Par le théorème des restes chinois, il existe un isomorphisme θ de l'anneau $\mathbb{Z}_n$ sur l'anneau produit

$$\mathbb{A} = \mathbb{Z}_{p_1^{e_1}} \times \dots \times \mathbb{Z}_{p_r^{e_r}}$$

L'isomorphisme θ induit un isomorphisme de groupes de $\mathbb{Z}_n^\times$ sur le groupe des inversibles de $\mathbb{A}$, qui est

$$G = G_1 \times \dots \times G_r = \mathbb{Z}_{p_1^{e_1}}^\times \times \dots \times \mathbb{Z}_{p_r^{e_r}}^\times$$

Proposition 2. *On suppose que n est un nombre de Carmichael. Alors, pour tout $i \in \llbracket 1, r \rrbracket$, $e_i = 1$ et $p_i - 1$ divise $n - 1$.*

Démonstration. Par l'isomorphisme θ , on a pour tout $x \in G$, $x^{n-1} = 1$. Et donc, pour tout $i \in \llbracket 1, r \rrbracket$, pour tout $x_i \in G_i$, $x_i^{n-1} = 1$. Le cardinal de G_i est

$$\varphi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$$

Nous allons ici admettre un résultat non trivial : le groupe G_i est cyclique. Prenons pour x_i un générateur de G_i . Les seules puissances de x_i égales à 1 sont les multiples du cardinal de G_i , donc $p_i^{e_i-1}(p_i - 1)$ divise $n - 1$.

Supposons que $e_i \geq 2$. Alors, p_i divise $n - 1$. Mais p_i divise n , donc p_i divise $n - (n - 1) = 1$, contradiction. Ainsi, $e_i = 1$. De là, $p_i^{e_i-1}(p_i - 1) = p_i - 1$ divise $n - 1$. $\square$

3 Conditions suffisantes

Nous allons maintenant examiner la réciproque.

Proposition 3. *Soit $n \in \mathbb{N}^*$. On suppose que $n = p_1 \dots p_r$ où $r \geq 2$, les p_i sont des nombres premiers impairs distincts, et pour tout $i \in \llbracket 1, r \rrbracket$, $p_i - 1$ divise $n - 1$. Alors, n est un nombre de Carmichael.*

Démonstration. Comme $r \geq 2$, l'entier n est composé. Soit $a \in \mathbb{Z}_n^\times$. Soit $x = (x_1, \dots, x_r) = \theta(a) \in G$. On a

$$x^{n-1} = (x_1^{n-1}, \dots, x_r^{n-1})$$

Soit $i \in \llbracket 1, r \rrbracket$. Par le petit théorème de Fermat, $x_i^{p_i-1} = 1$. Et donc, comme $p_i - 1$ divise $n - 1$, $x_i^{n-1} = 1$. Ainsi,

$$\theta(a^{n-1}) = \theta(a)^{n-1} = x^{n-1} = (1, \dots, 1) = \theta(1)$$

De là, par l'injectivité de θ , $a^{n-1} = 1$. $\square$

Remarquons que l'entier r ne peut pas être égal à 2.

Proposition 4. *Les nombres de Carmichael possèdent au moins trois diviseurs premiers.*

Démonstration. Soit n un nombre de Carmichael. Supposons $n = p_1 p_2$ où p_1 et p_2 sont deux nombres premiers distincts. Écrivons

$$n - 1 = (p_1 - 1)p_2 + p_2 - 1$$

$p_1 - 1$ divise $n - 1$, donc $p_1 - 1$ divise $p_2 - 1$. De même, en écrivant $n = (p_2 - 1)p_1 + p_1 - 1$, on obtient que $p_2 - 1$ divise $p_1 - 1$. De là, $p_1 - 1 = p_2 - 1$, d'où $p_1 = p_2$. Contradiction. $\square$

4 Bilan et compléments

4.1 Le critère de Korselt

Nous avons finalement montré le résultat suivant, appelé le *critère de Korselt* (1899).

Théorème 5. *Soit n un entier impair différent de 1. L'entier n est un nombre de Carmichael si et seulement si*

- n n'a pas de facteur carré.
- Pour tout diviseur premier p de n , $p - 1$ divise $n - 1$.

4.2 Une autre caractérisation

Le petit théorème de Fermat s'énonce parfois de la façon suivante : si n est un nombre premier, alors pour tout $a \in \mathbb{Z}_n$, $a^n = a$. Cette propriété reste-t-elle vérifiée par les nombres de Carmichael ? La réponse est affirmative.

Proposition 6. *Soit n un entier impair composé différent de 1. L'entier n est un nombre de Carmichael si et seulement si pour tout $a \in \mathbb{Z}_n$, $a^n = a$.*

Démonstration. Supposons que pour tout $a \in \mathbb{Z}_n$, $a^n = a$. Soit $a \in \mathbb{Z}_n^\times$. En multipliant par a^{-1} , on obtient $a^{n-1} = 1$, donc n est un nombre de Carmichael.

Inversement, supposons que n est un nombre de Carmichael. Soit $a \in \mathbb{Z}_n$. Écrivons $n = p_1 \dots p_r$ où $r \geq 3$ et les p_i sont des nombres premiers impairs distincts deux à deux. Reprenons l'isomorphisme θ . On a

$$\theta(a) = (x_1, \dots, x_r)$$

où, pour tout $i \in \llbracket 1, r \rrbracket$, $x_i \in \mathbb{Z}_{p_i}$. Si $x_i \in \mathbb{Z}_{p_i}^\times$ alors, par le petit théorème de Fermat, $x_i^{p_i-1} = 1$. Comme $p_i - 1$ divise $n - 1$, $x_i^{n-1} = 1$. En multipliant par x_i , il vient $x_i^n = x_i$. Sinon, $x_i = 0$ donc $x_i^n = 0 = x_i$. Ainsi,

$$\theta(a^n) = \theta(a)^n = (x_1^n, \dots, x_r^n) = (x_1, \dots, x_r) = \theta(a)$$

Par l'injectivité de θ , $a^n = a$. $\square$

4.3 Une majoration des diviseurs premiers d'un nombre de Carmichael

Proposition 7. *Les diviseurs premiers d'un nombre de Carmichael n sont strictement inférieurs à $\sqrt{n}$.*

Démonstration. Soit p un diviseur premier de n . On a

$$\frac{n/p - 1}{p - 1} = \frac{n - 1}{p - 1} - \frac{n}{p} \in \mathbb{N}$$

De là, $p - 1$ divise $n/p - 1$, donc $p - 1 \leq n/p - 1$ ou encore $p^2 \leq n$. De plus, $p^2 \neq n$ puisque n n'a pas de facteur carré. $\square$

Remarquons que cette propriété redémontre qu'un nombre de Carmichael a au moins trois facteurs premiers. En effet, si $p_1 < \sqrt{n}$ et $p_2 < \sqrt{n}$, alors $p_1 p_2 < n$, donc $n \neq p_1 p_2$.

4.4 Existe-t-il beaucoup de nombres de Carmichael ?

En 1994, W.R. Alford, Andrew Granville et Crandall Pomerance ont démontré qu'il existe une infinité de nombres de Carmichael. En notant $C(x)$ le nombre de nombres de Carmichael inférieurs à x , on a pour tout x assez grand

$$C(x) > x^{2/7}$$

On connaît de meilleurs minorants que celui-ci. En 2008, Harman a montré que l'on peut prendre $1/3$ pour l'exposant.

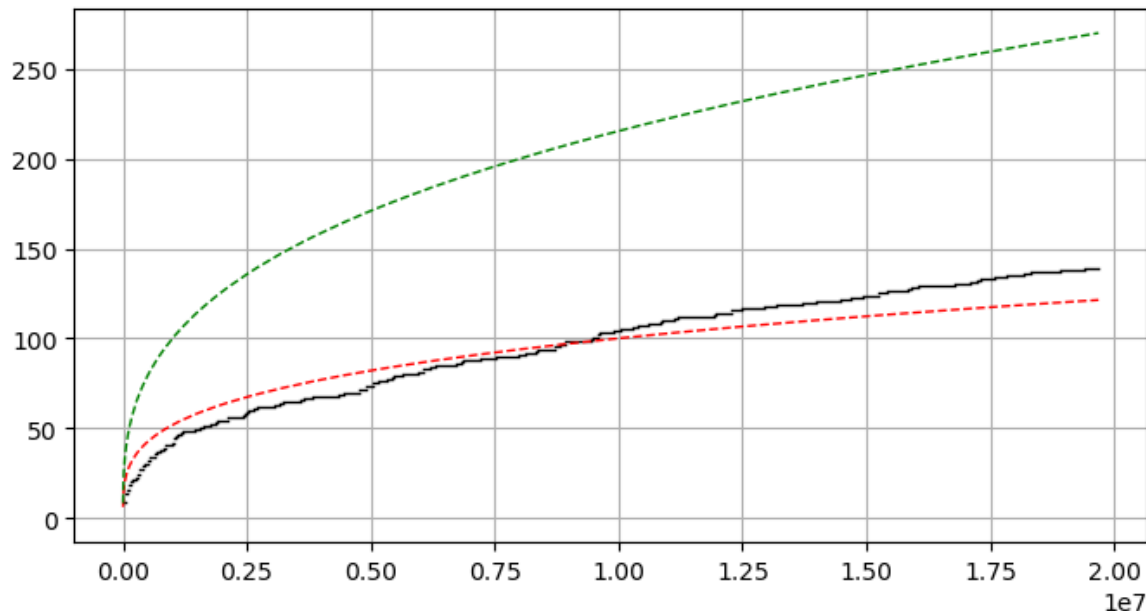


FIGURE 1 – En noir, $C(x)$. En rouge, $x^{2/7}$. En vert, $x^{1/3}$.

On voit sur la figure la courbe noire et la courbe rouge se croiser. En appelant C_k le k^e nombre de Carmichael (on démarre à $C_0 = 561$),

$$C_{96} = 8719921 < 96^{2/7} \quad \text{et} \quad C_{97} = 8830801 > 97^{2/7}$$

Bien évidemment, ceci ne prouve pas le théorème d'Alford, Granville et Pomerance. Les deux courbes pourraient à nouveau se croiser, se décroiser, se recroiser, etc. Quant à la courbe verte, le résultat de Harman montre que pour tout x assez grand, elle se trouve au-dessous de la courbe noire. Le « assez grand » signifie sûrement « vraiment très grand ».

Bibliographie.

La bibliographie sur les nombres de Carmichael est vaste. Les références ci-dessous peuvent être trouvées en ligne. Les trois premières sont des articles fondateurs sur la question.

- R.D. Carmichael, Note on a New Number Theory Function, Bulletin Amer. Math. Soc. 16 (1910), pp 232–238.
- R. D. Carmichael, On composite P which satisfy the Fermat congruence $a^P - 1 \equiv 1 \pmod{P}$, Amer. Math. Monthly 19 (1912), pp. 22–27.
- W.R. Alford, Andrew Granville, Crandall Pomerance, There are infinitely many Carmichael numbers, Annals of Mathematics, 140 (1994), pp 703-722.
- Keith Conrad, Carmichael numbers and Korselt's criterion.
- Victor Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press (2008).